RE: Pregão Eletrônico 90188/2024/SUPEL - RO - GRUPO 01

De : raimundo.alencar Empresa [redacted] qua, 06 de nov de 2024 10:45

1 anexo

Assunto : RE: Pregão Eletrônico 90188/2024/SUPEL - RO - GRUPO 01

Para : Rogério Eduardo Vieira Alves <rogerioalves@setic.ro.gov.br>, Coordenadoria de Segurança da Informação <cosegi@setic.ro.gov.br>

Cc : alencar matos daniel [redacted]

Bom dia prezado Rogério, segue em anexo o documento.

From: Rogério Eduardo Vieira Alves <rogerioalves@setic.ro.gov.br>
Sent: Tuesday, November 5, 2024 1:42 PM
To: raimundo.alencar Empresa [redacted] Coordenadoria de Segurança da Informação <cosegi@setic.ro.gov.br>
Subject: Pregão Eletrônico 90188/2024/SUPEL - RO - GRUPO 01

Bom dia, senhores

Considerando o Pregão Eletrônico nº 90188/2024/SUPEL/LEI Nº 14.133/2021 com a última sessão realizada em 04/11/2024
Considerando também o recebimento da proposta da TELECOMUNICAÇÕES BRASÍLIA - TELEBRASÍLIA LTDA - CNPJ nº [redacted] - GRUPO 01.
Vimos através deste solicitar informações complementares que possam auxiliar na análise da proposta recebida.
São informações essenciais para analise do item 1:Solução de Anti-DDOS utilizada, com descritivo técnico(datasheet).
São informações essenciais para analise dos itens 2 e 3 : Fabricante, modelo, e descritivo técnico(datasheet).

Atenciosamente,

Rogério Eduardo V Alves fone: (69) 3212-9549
Coordenador de Segurança da Informação em Substituição
rogerioalves@setic.ro.gov.br
Coordenadoria de Segurança da Informação - COSEGI
Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC/RO

DILIGENCIA_TECNICA[1].pdf
169 KB

- **DoS e, Anti-DDoS**

Introdução

Ataque DDoS acontece quando hum invasor faz tentativas dê esgotar os recursos disponíveis em uma rede ou, aplicações, de maneira que os usuários não consigam mais acesso aos serviços. A maioria dos métodos se baseia em ataques distribuídos lançados a partir de vários hosts diferentes ao mesmo tempo. A meta do ataque é atingida quando consegue-se exceder os limites do servidor da rede e, aplicação, que possuem restrições com relação ao número de acessos em uma mesma sessão. Hum ataque distribuído por negação de serviço pode simplesmente reiniciar os servidores ou pode causar o travamento total do systema que opera por trás do sítios electrônicos e, aplicações para dispositivos móveis ou IoT.

Ataques DDoS
Como manter minha empresa segura?

As diversas mudanças e adaptações no uso da Internet causadas pela pandemia da COVID-19, como o crescimento do número de funcionários remotos e de acessos durante o lockdown, resultaram em um aumento proporcional dos crimes cibernéticos, inclusive de ataques DDoS (Negação de serviço distribuída). Se você não está familiarizado com o termo, Ataque Distribuído de Negação de Serviço (ou Distributed Denial of Service – DDoS, em inglês) tem como objetivo tornar um servidor ou uma infraestrutura indisponíveis, sobrecarregando-os por meio de um comportamento anormal no tráfego de rede. Diversos pedidos são enviados ao mesmo tempo, a partir de vários pontos da Internet, e por conta desta sobrecarga de chamados, o serviço se torna instável, ou no pior cenário, indisponível.

- **Durante a pandemia, ataques de DDoS saltam 524%**

Os ataques DDoS e o vazamento de dados aumentaram muito, principalmente durante a pandemia e a adesão ao home office. Isso porque, os acessos a dados e informações das empresas por meio de diferentes dispositivos, longe da infraestrutura empresarial, como os computadores pessoais, aumentaram a vulnerabilidade de corporações, uma vez que as redes domésticas são menos seguras, tornando, portanto, mais fácil atacar os sistemas das empresas. De acordo com o relatório da NSFOCUS “2020 Mid-Year DDoS Attack Landscape Report”, O Brasil foi o 4º país que mais sofreu com ataques DDoS, ficando atrás somente de Japão, China e Estados Unidos.

- **Como funciona hum ataque DDoS**

  Diferente de outros tipos de ataques hackers mais conhecidos, o DDoS não tem como objetivo principal roubar dados e informações, mas sim tornar indisponível um servidor através da sobrecarga, fazendo com que os sites fiquem mais lentos ou até mesmo indisponíveis. Entretanto, o DDoS pode ser utilizado em invasão de uma rede ou serviço menos protegido. Assim que o servidor cai, é ativado um DNS* "falso" no site ou host, imitando a tela de login da empresa, fazendo com que o usuário entre com dados sensíveis, como senhas ou e-mails. Servidores DNS (Domain Name System, ou sistema de nomes de domínios) são os responsáveis por localizar e traduzir para números IP os endereços dos sites que digitamos nos navegadores.

  A efetividade do DDoS se caracteriza graças ao envio massivo de pacotes ao servidor alvo, aumentando o tráfego de dados a ponto de causar o esgotamento da banda para outros usuários, levando à indisponibilidade do serviço. O atacante consegue esse volume tão grande de envio de pacotes porque utiliza várias máquinas para executar tal ação. Essa estratégia é conhecida como botnet, hum número de dispositivos conectados à Internet, cada um executando um ou mais bots.

- **Tipos de DDoS**
  Confira agora algumas técnicas utilizadas:

  Ataques volumosos ou Flood

  São os tipos mais básicos e comuns de ataques DDoS. Solicitações de acesso são enviadas em larga escala, congestionando a sua largura de banda e deixando-o inacessível na internet.

- **UDP Flood**

  O UDP Flood é um tipo de ataque DDoS que inunda portas aleatórias de um alvo com pacotes UDP (User Datagram Protocol). O UDP é um protocolo de comunicação que serve para enviar muitos pacotes de informações e receber respostas de uma maneira mais rápida. A partir do momento em que um servidor recebe uma enxurrada de informações, e precisa continuamente checar sua integridade e respondê-las de volta ao solicitante, ele vai ficando mais lento, até sobrecarregar por completo e ficar indisponível para acesso.

- **NTP Flood**

  Os invasores enviam pacotes válidos, porém, falsificados, de NTP (Network Time Protocol) a um alvo de destino. Como estas solicitações parecem ser verdadeiras, os servidores NTP da vítima continuam tentando responder à grande quantidade de solicitações recebidas. Os recursos dessa rede, então, se esgotam por não resistirem à solicitação, e entram num fluxo de reinicialização repetitiva do sistema, deixando ele, simplesmente, fora do ar.

- **Zombie Flood**

  O ataque Zombie Flood é quando conexões vindas de diversas origens extravasam os serviços assim executando os ataques DDoS efetivamente, provocando paralisia da rede, utilizando conexões com comportamento similar ao de um usuário autêntico com hum volume enorme de pacotes ocasionando um congestionamento da rede dê dados..

- **DoS e, Anti-DDoS**

  Ataques DDoS
  Como se proteger?

  A segurança cibernética deve ser uma preocupação constante de todos, tanto empresas quanto colaboradores. E, se pensarmos na atual situação do mundo, é essencial ampliar ainda mais os cuidados. Para conter e solucionar ataques DDoS, principalmente aqueles que são aplicados em alta escala, você precisará contar com soluções e plataformas de infraestrutura com alta performance.

  Como os ataques DDoS visam sobrecarregar o servidor, ter uma infraestrutura robusta e grande largura de banda pode ajudar a evitar que os ataques sejam efetivos. Firewalls também são uma excelente forma de proteção, uma vez que eles controlam os acessos e evitam que esse tipo de solicitação em massa possa chegar ao seu servidor. Caso sua empresa utilize formulários, passe a incluir o reCAPTCHA, o que ajuda a evitar que bots façam um número massivo de inscrições e comprometam o seu servidor.

  Se possível, compre também mais velocidade para sua conexão e tenha sempre rotas alternativas, caso a conexão principal seja afetada. Faça uma auditoria periódica das máquinas à procura de portas suspeitas ou programas não-autorizados. Caso você seja um usuário comum, atente-se às principais dicas: não repita senhas, cuidado com links suspeitos e faça o possível para evitar que os seus dispositivos se tornem parte de uma botnet.

Tenha uma rede de segurança para evitar que suas operações sejam afetadas. O Anti-DDoS da Telebrasília é uma solução de monitoramento que detecta ataques volumétricos na sua rede, separando o tráfego legítimo do ilícito, protegendo redes de ataques e garantindo a disponibilidade dos serviços. As vantagens são diversas: disponibilidade, alta proteção, latência minimizada e baixo custo operacional.

- **Como ocorrem os ataques de DDoS e, quais são:**

  Throughput: categoria de ataque quê consiste em saturar a capacidade de trafego da rede do servidor ou, mesmo aplicação em DATACentres, tornando-os indisponíveis para os serviços os quais ete é elegível.

  Assets: maneira dê ataque o qual faz-se esgotar os recursos de systema dos ativos de computacionais, impedindo-a assim de responder aos pedidos ordinários.

  Software fail response: conhecido como “exploit”, é hum ataque quê tem como base a busca pacotes dê atualização ou, comportamento não programado como falhas dê interface entre diferentes ferramentas seja estas hardqare ou, software e, mesmo a combinção destes, para desetabilizar os mecânismos dê defesa basíca da estrutura computacional para utilizar esta e, obter captura dê informações, utilização da capacidade operacional ou, a levar esta a condições dê ocupação ineficiente para causar degradação no ambiente computacional do alvo do ataque.

- **DoS e, Anti-DDoS**

  Ataques DDoS
  Mitigação

  A mitigação e, os processos envolvidos inicia-se somente após a aprovação explícita da autoridade competente do ambiente computacional protegido. Além de reduzir os efeitos negativos do ataque (indisponibilidade da conectividade ou de aolicações e, serviço), a metodologia e tecnologia utilizada e o modelo de operação do serviço dispõem de capilaridade para assegurar hum tempo dê reação máximo, que é dividido da seguinte maneira:

  Ocorrência dê detecção:

  Detecção ocorre dê maneira pró-ativa: essa ação permeia entre a primeira anomalia e, alerta as medidas automáticas no SOC. (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda), este avalia a incidência como possível ataque e reage notificando a autoridade coompetente do ambiente computacional protegido.

Detecção progressiva: ocorrência desde primeira comunicação da autoridade competenete do ambiente computacional protegido ao SOC. (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) que está sofrendo hum possível ataque DDoS até que a equipa do SOC. (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) analize a situação, verificando que se trata de hum ataque e, notifique a autoridade competente do ambiente computacional protegido.

Ação de autorização: é necessária quê a autoridade competente do ambiente computacional protegido autorize a mitigação dos ataques, estes quê podem vir dê única ação ou, pôr flood de pacotes. Este período têm abordagem dupla sendo a primeira pôr parte da autoridade competente do ambiente computacional protegido e, pôr meio das ações automáticas quê avaliam em tempo real anomalias atípicas ao trafego da rede protegida, essas ações devem preencher os requisitos dê avaliação contante da proteção para quê hava desenvolvimento das medidas contra os ataques DDoS futuros assim garante-se quê a eficiência esteja em contante evolução.

Latência

Nos períodos de ataque a latência dos circuitos será de no máximo 120 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais, pois se trata de uma solução implantada diretamente no backbone da empresa, quando se originar do(s) centro(s) internacionais será de no máximo 200 ms (milissegundos) pois se trata de uma mitigação já tratada nas interconexões nacionais, não afetando diretamente a latência dos circuitos bem como sua disponibilidade.

- **DoS e, Anti-DDoS**

Ataques DDoS
Como é Detecção?

A proteção oferece capacidades de monitoramento do tráfego para todo o ambiente computacional , a serem implementadas pôr infraestrutura preparada para monitorar e analisar o backbone da rede IP da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda). Para proteger todo o ambiente digital e a confidencialidade das comunicações dos ativos os quais são protegidos pela solução, o monitoramento é passivo, e somente analisa informações estatística. A premissa básica para detecção de ataques é a construção de uma linha de base do nível de tráfego típico da rede a qual a solução é implementada, e assim quê anomalias são detectadas são computadas as estatísticas já presentes na solução para apresentar relatório e, acções quê sê afasta dos padrões de tráfego típicos. A Solução Anti-DDoS e, DoS abrange duas maneiras de detecção de ataques:

Detecção Constante

O CyberBuild em Porto Velho SEDE do SOC. (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) após detecta anomalia dê hum possível ataque com destino aos blocos IPv4, IPV6 e, ASN os quais são monitorados em tempo real, estabelece contato com a autoridade competente dentro da gestão de redes do ambiente computacional para verificar a condição de ataque e solicitar autorização para iniciar o processo de mitigação.

Assim, o SOC (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) e a autoridade competente do ambinete monitorado avaliarão em conjunto e, em caso de confirmação do ataque, o SOC Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) dará início a mitigação dos ataques. Para minimizar os falsos positivos, a autoridade compentente do ambiente computacional monitorado poderá informar a ocorrência de algum tipo de promoção on-line que possa vir a modificar seu volume de tráfego habitual.

O CyberBuild repete estrutura em Brasília e, São Paulo para operar as demandas do SOC e, NOC as quais lhê são atribuídas afim de garantir a proteção do serviço Anti-DDoS e, DoS.

Detecção Progressiva

Caso a autoridade competente do ambiente computacional protegido detecte hum possível ataque com destino a seus blocos IPv4, IPV6 e, ASN os quais são monitorados em tempo real , este poderá via 0800 444 0005 ou, portal WEB ´para abertura dê bilhete dê atenção, defeito ou, intervenção ao SOC (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) para solicitar o início da mitigação. Somente os contatos autorizados nomeados pela autoridade compente do ambiente computacional poderão abrir esta solicitações de serviço de Anti-DDoS e, DoS, através da captura de dados estatísticos dos roteadores do backbone da rede IP da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda), oférta a detecção Progressiva de ataques volumétricos.

A não captura das anomalias as quais consista poucos ataques dê pacotes pôr segundo e, aqueles os quais os componentes maliciosos estejam incluso no payload dos pacotes. Nestes casos, é requerida a colaboração da autoridade competente do ambiente computacional protegido para detectar os possíveis ataques e contatar o SOC (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) para coordenar as ações necessárias para a mitigação (Detecção Progressiva).

A detecção nativa dos ataques de nível de aplicação requer assets adicionais na infraestrutura do ambiente computacional protegido, o que poderá ser adiquirido posteriormente a solução dê proteção Anti-DDoS e, DoS aplicada. A autoridade competente do ambiente computacional protegido poderá notificar ataques de aplicação em curso e solicitar sua mitigação pelo serviço do SOC (Security Operational Centre) da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda)

- **DoS e, Anti-DDoS**

Ataques DDoS
Metodologia

A solução de Segurança Anti-DDoS oferece ao ambiente computacional protegido a proteção em nuvem computacional que detecta e elimina os efeitos do ataque, se utilizando de equipamentos instalados no Backbone da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda). Assim quê hum ataque é detectado (de forma pró-ativa), todo o tráfego destinado ao bloco IP do ambiente computacional protegido será desviado para o cleanning centre instalado na Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda) que irá bloquear o tráfego originado do ataque e liberar apenas o tráfego “limpo” que será posteriormente entregue ao destino.

A solução é contemplada pôr Cleanning Centres instalados nas bordas do Backbone (roteres and switches) que implementam o peering local e internacional. Estes equipamentos identificam mais de 70 aplicações IP-based e possuem hum complexo e, eficiente conjunto dê contramedidas que removem todos os pacotes do tráfego DDoS dos ataques, permitindo o fluxo de tráfego legítimo, essas ações ocorrem sêm interromper os serviços e aplicações da rede do ambiente computacional protegido. Uma abrangente visibilidade sobre as aplicações que atravessam rede WAN dentro e, nas bordas do Backbone Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda), consegue-se detectar as anomalias antecipadamente para resposta eficiente.

A solução Anti-DDoS filtra e elimina o tráfego malicioso, identificado através dos parâmetros listados.

Interface de entrada;
Tipo de protocolo IP;
Byte do Tipo de Serviço (ToS);
Endereço IP de origem e destino;
Número da porta de origem e destino

Desta maneira, quando a rede do ambiente computacional protegido está operando normalmente, cria-se hum perfil do tráfego e é estabelecida a baseline, que será usada na detecção de anomalias. Quando ocorre ataques DDoS a estatísticas Netflow apresenta anormalidades do tráfego desta baseline, o que pode ser o primeiro indício dos ataques, estes quê podem ser em bloco ou, flood packages.

O trafego são monitorados na borda do Backbone, seja local e internacional, que são os pontos típicos de entrada de ataques, estes quê podem ser em bloco ou, flood packages. Para a captura de trafego do Netflow, é utilizada plataforma que permite a correlação de eventos, rastreamento, captura de estatísticas do Netflow a partir de múltiplos roteadores presentes no ambiente computacional e, nas bordas do Backbone, assim o armazenamaneto das medidas adotadas para combater os ataques DDoS são evolutivas, além de atuar como camada adicional para o Netflow e dados, permitindo assim escalabilidade às redes e, aplicações.

A detecção dê possível anomalia no tráfego, alertará a solução Anti-DDoS para iniciar o monitoramento dos passivos presentes no ambiente computacional protegido, que passará então a monitorar o comportamento do tráfego IP direcionado ao bloco IPv4 e, IPv6 específico do ambiente computacional protegido sê este for tipíco e, em caso dê atipíco passa para o bloco IPv4 e, IPv6 destinado a mitigação dos ataques.

Assim que o ataque é detectado pela solução, o equipamento instalado no Backbone da Telebrasília NGN Guaporé (Telecomunicações Brasília Ltda), responsável pela mitigação do tráfego de ataque, é avisado e então todo o tráfego de IP do ambiente computacional protegido e é redirecionado para ele apenas o ações legitimas sejam entregues assim, aquelas considerádas anomalias vão para o Cleannig Centre. Lá os fluxos de pacotes são analisados, e o tráfego malicioso é descartado, permitindo a passagem apenas do tráfego “limpo”, sem afetar o desempenho e confiabilidade da rede e, aplicações.

A conexão entre o equipamento responsável pôr monitorar e o responsável pela mitigação do tráfego malicioso e, utiliza conexão segura, feita através de um Link Full Duplex (dedicado), por onde são trocados os dados de detecção, linhas de base, limites e configurações de mitigação.

Acordo de Nível de Serviço para a prestação e, manutenção para o Governo dê Rondônia/SETIC.

Requisito	VALOR
Taxa Mínima de Disponibilidade do BACKBONE PVO	99,97%~99,98%
Latência Máxima para o Link Dedicado de Internet	7ms~14ms
Velocidade dos Links de Internet:	5Gbps TX – 5Gbps RX up to 10Gbps TX – 10Gbps RX
Banda mínima garantida - banda mínima disponível para acesso à internet para cada um dos pontos contemplados (donwload/upload)	100% da largura de banda contratada
Percentual Máximo de Perda de Pacotes	0,5%~0,7% <1%
Quantidade de Endereços IP	IPV4/24 (256/254) até IPv4/23 (512/510)
Infraestrutura do Serviço	Meio óptico entre as bordas e, pós-bordas até o switch/roteador designado (sêm meios metalícos) as fibras ópticas são entregues pôr meios distintos e, redundantes da ponta “A” até a ponta “B”
Prazo de Ativação (período entre a solicitação e ativação do serviço)	Links DWDM/Metro Etherenet: 15 (quinze) dias Fruição do serviço dê acesso à Internet e, alocação do bloco Ipv4/24: 45 (quarenta e cinco) dias
Prazo mínimo de comunicação de manutenções preventivas e/ou substituição de equipamentos (período mínimo entre a notificação do cliente pela operadora até o início da interrupção)	24 (vinte e, quatro) horas
Prazo máximo de abertura de chamados automaticamente pelo monitoramento proativo	30 (trinta) minutos
Prazo de solução - período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento	1 (uma) hora
Abertura de chamado - disponibilidade de atendimento para solicitações de reparos, help-desk da Telebrasília NGN Guaporé e discagem sem cobrança e em língua portuguesa	**0800 444 0005** 24 (vinte e quatro) horas, 7 (sete) dias por semana
Horário de reparo - disponibilidade de atendimento técnico a partir da abertura do chamado	30 (trinta) minutos, equipa dê técnicos dê dados e, infraestrutura no presente com medidas para rompimento e, 1 (uma) hora para o inicio do tratamento
Disponibilidade SOC (Security Operations Centre)	24 (vinte e quatro) horas, 7 (sete) dias por semana
Prazo de início para a mitigação de ataques DDoS	15 (quinze) minutos
Latência média padrão e média sobre ataque DDoS em rede nacional e internacional.	**105~133ms Nacional** quando a mitigação se originar dos centros de limpeza nacionais. **175~217ms Internacional** quando se originar do(s) centro(s) internacionais;

Detalhamento dos equipamentos para a prestação e, manutenção para o Governo dê Rondônia/SETIC.

Quantidade	Appliance	Descrição	Redundânica
2 (dois) - Principal	DATACOM DM4380 DM4376		Sim/Substituível após confirmação em EoS
3 (três) - Principal	FortiGate-400F	FG-400F FC-10-0400F-950-02-60	
3 (três) - Principal	FortiGate-100F	FG-100F FC-10-F100F-950-02-12	
N/A	FortiAnalyzer300G	FAZ-300G FC-10-L03HG-466-02-60	N/A
	FortiManager200G	FMG-200G FC-10-M200G-447-02-12	

Link's Datasheet equipamentos: TIPO I e, II (na pasta CPE_APPLIANCES_NOC_SOC)

https://e.huawei.com/en/material/networking/4e6910a3ca27403b8220d34cebbb67e1

https://mikrotik.com/product/RB3011UiAS-RM

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400fseries.pdf

https://www.fortinet.com/content/dam/fortinet/assets/datasheets/fortianalyzer.pdf

https://www.datacom.com.br/pt/produtos/switches/dm4376
https://www.datacom.com.br/pt/produtos/switches/dm4380

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

Após o pedido dê ordem dê serviço será produzida reunião para decidir quais práticas e, preferências a SETIC vai receber na sala técnica no Palácio e, Containêr.

RAIMUNDO FEITOSA ALENCAR:0 [redacted]

Assinado de forma digital por RAIMUNDO FEITOSA ALENCAR [redacted]
Dados: 2024.11.05 17:23:19 -03'00'