DESCRIPTOGRAFIA E INSPEÇÃO DE TRÁFEGO CRIPTOGRAFADO

Proteção de alto desempenho contra uso mal-intencionado de criptografia

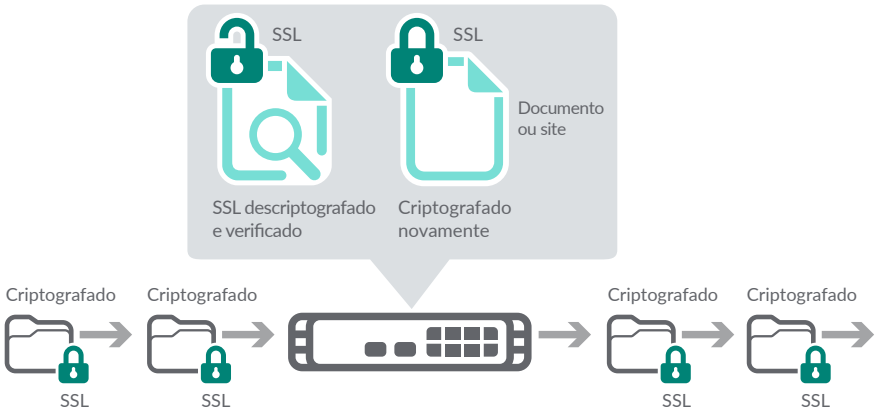
De acordo com o Relatório de Ameaças Cibernéticas da SonicWall de 2018, o tráfego criptografado agora representa quase setenta por cento da comunicação total pela Web de uma organização. Embora haja muitos benefícios em criptografar sessões da Internet, como proteger a privacidade e a integridade de informações pessoais para a troca de dados, observamos o surgimento de uma tendência menos positiva à medida que criadores de malware exploram esse recurso de criptografia como uma maneira de ocultar seus ataques dos firewalls. Os invasores podem não apenas transpassar os firewalls e aproveitar os pontos cegos para introduzir malware que abrem portas diretamente para qualquer rede, como também utilizam TLS/SSL para ocultar comandos e controlar o tráfego para manipular sistemas comprometidos de praticamente qualquer lugar. As organizações que não inspecionam o tráfego criptografado perdem grande parte do valor de seus sistemas de firewall. Elas são incapazes de visualizar o que está dentro daquele tráfego, reconhecer downloads de malware, identificar arquivos danosos ou ver a transmissão não autorizada de informações privilegiadas para sistemas externos.

As organizações podem proteger suas redes contra esses riscos de segurança por meio de uma combinação de tecnologias de prevenção contra ameaças baseadas em nuvem e prontas para uso. Para aprimorar o serviço Capture Advanced Threat Protection (ATP) com múltiplos mecanismos da SonicWall, temos a nossa tecnologia Real-Time Deep Memory Inspection (RTDMI™) com patente pendente. O mecanismo RTDMI detecta e bloqueia de forma proativa malware em grande escala, ameaças zero-day e malware desconhecido ao inspecionar a memória diretamente. Devido à arquitetura em tempo real, a tecnologia SonicWall RTDMI é precisa, minimiza falsos positivos, além de identificar e mitigar ataques sofisticados em que as armas do malware são expostas por menos de 100 nanossegundos. Em conjunto, o mecanismo patenteado* Reassembly-Free Deep Packet Inspection (RFDPI) de uma única passagem da SonicWall examina cada byte de cada pacote, inspecionando o tráfego de entrada e saída no firewall.

O DPI-SSL fornece segurança, controle de aplicações e prevenção contra vazamento de dados críticos para analisar HTTPs e outros tráfegos criptografados por TLS/SSL.

Benefícios:

- Obtenha visibilidade do tráfego criptografado por TLS / SSL
- Obtenha prevenção contra ameaças de ponta com as tecnologias Real-Time Deep Memory Inspection e Reassembly-Free Deep Packet Inspection
- Bloqueie downloads de malware oculto
- Impeça comunicação C&C e exfiltração de dados
- Personalize listas de inclusão e exclusão para exigências de conformidade ou legais



Como uma camada ou proteção adicional, o SonicWall Deep Packet Inspection of TLS/SSL (DPI-SSL) fornece proteção avançada contra ameaças criptografadas com o uso do mecanismo Reassembly-Free Deep Packet Inspection patenteado da SonicWall, que verifica uma matriz ampla de protocolos de criptografia, inclusive HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS e POPS, independentemente da porta utilizada.

O DPI-SSL descriptografa o tráfego TLS/SSL, inspeciona-o em busca de ameaças, volta a criptografá-lo e o envia ao seu destino, caso nenhuma ameaça ou vulnerabilidade seja encontrada. É um serviço muito importante que fornece segurança e controle de aplicações críticos, além de evitar o vazamento de dados.

Recursos

Alto desempenho e contagem de conexões: os firewalls de última geração da SonicWall utilizam uma arquitetura de processador avançada e um número muito alto de conexões para aprimorar o desempenho e a proteção DPI-SSL em todos os dispositivos conectados.

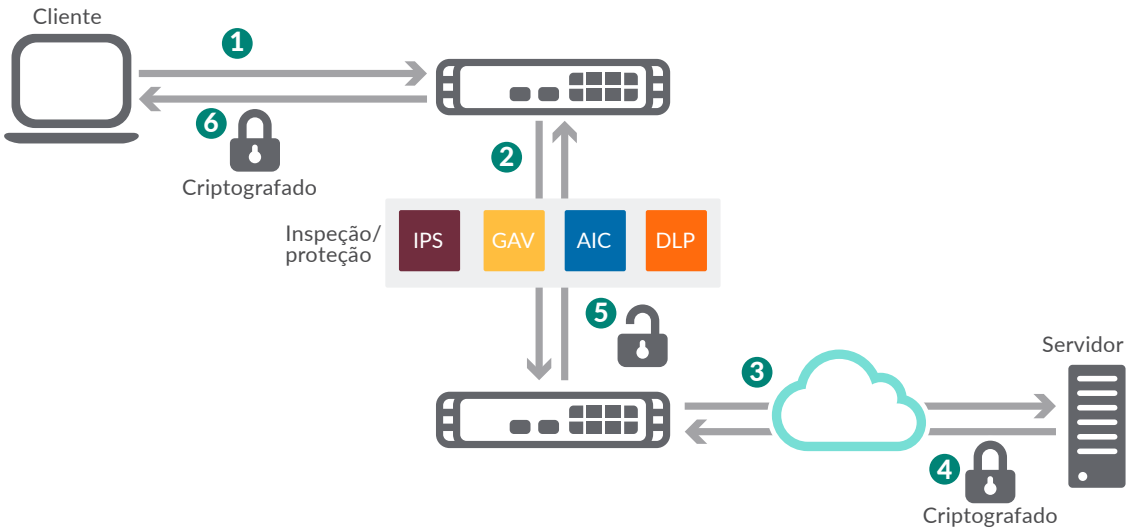
Configuração simples e segura: a descriptografia e a inspeção DPI-SSL protegem os usuários na rede com configuração e complexidade mínimas.

Lista de inclusão/exclusão: para implementações de tráfego intenso, os administradores podem excluir fontes confiáveis para maximizar o desempenho da rede. Além disso, os administradores podem direcionar tráfego específico para inspeção de TLS/SSL ao personalizar uma lista que especifique endereço, serviço ou objetos ou grupos de usuários para conformidade com exigências de privacidade e/ou legais.

Modo de implementação do cliente: inspeciona o tráfego TLS/SSL quando o cliente está na LAN do firewall e acessa conteúdo localizado na WAN. Depois que o appliance tiver descriptografado e inspecionado o tráfego criptografado, ele reescreverá o certificado enviado pelo servidor remoto e assinará o certificado recém-gerado com o certificado especificado pelo usuário. Por padrão, essa é a autoridade de certificação (CA) do appliance, embora seja possível selecionar um certificado diferente.

Modo de implementação do servidor: inspeciona o tráfego TLS/SSL quando clientes remotos se conectam por meio da WAN para acessar o conteúdo localizado na LAN do firewall, o que permite que o administrador configure correspondências entre um objeto de endereço e um certificado. Quando o appliance detecta conexões TLS/SSL para o objeto de endereço, ele apresenta o certificado correspondente e negocia TLS/SSL com o cliente que está em processo de conexão. Neste cenário, o proprietário do firewall de última geração da SonicWall detém os certificados e as chaves privadas dos servidores de conteúdo de origem.

Suporte abrangente: o suporte inclui prevenção contra intrusão, prevenção contra malware, controle de aplicações, filtragem de conteúdo/URL e prevenção contra comunicação de comando e controle de malware.



Inspeção TLS/SSL - Modo de implementação do cliente

1. O cliente inicia o handshake de TLS/SSL com o servidor
2. O NGFW intercepta a solicitação e estabelece a sessão com o uso de seus próprios certificados no lugar do servidor
3. O NGFW inicia o handshake de TLS/SSL com o servidor em nome do cliente com o uso do certificado TLS/SSL definido pelo administrador
4. O servidor conclui o handshake e cria um túnel protegido entre ele e o NGFW
5. O NGFW recriptografa o tráfego e o envia ao cliente
6. O NGFW descriptografa e inspeciona todo o tráfego proveniente do cliente ou destinado a ele, para verificar se há ameaças e violações de política

Requisitos do sistema

A inspeção TLS/SSL está disponível com os firewalls de última geração da SonicWall seguintes:

FIREWALL	LICENÇA ÚNICA
SOHO/SOHO W	01-SSC-0723
TZ300/TZ300 W/TZ300P	Incluído na assinatura dos serviços de segurança
TZ400/TZ400 W	Incluído na assinatura dos serviços de segurança
TZ500/TZ500 W	Incluído na assinatura dos serviços de segurança
TZ600/TZ600P	Incluído na assinatura dos serviços de segurança
NS*a* 2650	Incluído na assinatura dos serviços de segurança
NS*a* 3650	Incluído na assinatura dos serviços de segurança
NS*a* 4650	Incluído na assinatura dos serviços de segurança
NS*a* 5650	Incluído na assinatura dos serviços de segurança
NS*a* 6650	Incluído na assinatura dos serviços de segurança
NS*a* 9250	Incluído na assinatura dos serviços de segurança
NS*a* 9450	Incluído na assinatura dos serviços de segurança
NS*a* 9650	Incluído na assinatura dos serviços de segurança
SuperMassive 9800	Incluído na assinatura dos serviços de segurança
NS*sp* 12400	Incluído na assinatura dos serviços de segurança
NS*sp* 12800	Incluído na assinatura dos serviços de segurança
NSv 10	Incluído na assinatura dos serviços de segurança
NSv 25	Incluído na assinatura dos serviços de segurança
NSv 50	Incluído na assinatura dos serviços de segurança
NSv 100	Incluído na assinatura dos serviços de segurança
NSv 200	Incluído na assinatura dos serviços de segurança
NSv 300	Incluído na assinatura dos serviços de segurança
NSv 400	Incluído na assinatura dos serviços de segurança
NSv 800	Incluído na assinatura dos serviços de segurança
NSv 1600	Incluído na assinatura dos serviços de segurança

Sobre nós

A SonicWall tem combatido o setor de crime cibernético há mais de 27 anos, ao defender pequenas, médias e grandes empresas em todo o mundo. Nossa combinação de produtos e parceiros possibilitou uma solução automatizada de detecção e prevenção de violação em tempo real ajustada às necessidades específicas de mais de 500.000 organizações em mais de 215 países e territórios, o que permite que você faça mais negócio com menos preocupações. Para obter mais informações, acesse www.sonicwall.com ou siga-nos no Twitter, no LinkedIn, no Facebook e no Instagram.

Serviços ativados por parceiros

Precisa de ajuda para planejar, implementar ou otimizar sua solução SonicWall? Os Parceiros de serviços avançados da SonicWall são treinados para fornecerem a você serviços profissionais de nível mundial. Saiba mais em www.sonicwall.com/PES.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte o nosso site para informações adicionais.
www.sonicwall.com

DataSheet-DecryptionAndInspection-US-VG-MKTG4334