IPsec 전송 중 암호화를 구성합니다

ONTAP 9

NetApp
February 12, 2026

목차

IPsec 전송 중 암호화를 구성합니다

ONTAP 네트워크에서 IP 보안 사용을 준비합니다

ONTAP 9.8부터 IP 보안(IPsec)을 사용하여 네트워크 트래픽을 보호할 수 있습니다. IPsec은 ONTAP에서 사용할 수 있는 여러 가지 데이터 이동 중 또는 전송 중 암호화 옵션 중 하나입니다. IPsec을 프로덕션 환경에서 사용하기 전에 구성할 준비를 해야 합니다.

ONTAP에서 IP 보안 구현

IPSec은 IETF에서 관리하는 인터넷 표준입니다. IP 레벨에서 네트워크 엔드포인트 간에 흐르는 트래픽에 대한 인증뿐 아니라 데이터 암호화 및 무결성을 제공합니다.

ONTAP를 통해 IPsec은 ONTAP와 NFS, SMB 및 iSCSI 프로토콜을 포함한 다양한 클라이언트 간의 모든 IP 트래픽을 보호합니다. 네트워크 트래픽은 개인 정보 보호 및 데이터 무결성 외에도 재생 및 메시지 가로채기 공격과 같은 여러 공격으로부터 보호됩니다. ONTAP는 IPsec 전송 모드 구현을 사용합니다. IPv4 또는 IPv6를 사용하여 ONTAP와 클라이언트 간의 키 자료를 협상하는 데 IKE(인터넷 키 교환) 프로토콜 버전 2를 활용합니다.

클러스터에서 IPsec 기능이 활성화된 경우 네트워크에는 다양한 트래픽 특성과 일치하는 ONTAP SPD(보안 정책 데이터베이스)에 하나 이상의 항목이 필요합니다. 이러한 항목은 데이터를 처리하고 전송하는 데 필요한 특정 보호 세부 정보(예: 암호 그룹 및 인증 방법)에 매핑됩니다. 각 클라이언트에는 해당 SPD 항목도 필요합니다.

특정 트래픽 유형의 경우 다른 이동 중인 데이터 암호화 옵션이 더 선호될 수 있습니다. 예를 들어, NetApp SnapMirror 및 클러스터 피어링 트래픽의 암호화를 위해 일반적으로 IPsec 대신 TLS(전송 계층 보안) 프로토콜을 사용하는 것이 좋습니다. TLS는 대부분의 상황에서 더 나은 성능을 제공하기 때문입니다.

관련 정보

- "Internet Engineering Task Force의 약어입니다"
- "RFC 4301: 인터넷 프로토콜에 대한 보안 아키텍처"

ONTAP IPsec 구현의 진화

IPsec은 ONTAP 9.8에서 처음 도입되었습니다. 이후 ONTAP 릴리스에서는 아래에 설명된 대로 구현 방식이 지속적으로 발전해 왔습니다.

ONTAP 9.18.1

IPsec 하드웨어 오프로드에 대한 지원이 IPv6 트래픽으로 확장되었습니다.

ONTAP 9.17.1

IPsec 하드웨어 오프로드에 대한 지원이 확장되었습니다. "링크 집계 그룹" . "포스트퀀텀 사전 공유 키(PPK)" IPsec 사전 공유 키(PSK) 인증이 지원됩니다.

ONTAP 9.16.1

암호화 및 무결성 검사와 같은 여러 암호화 작업을 지원되는 NIC 카드로 오프로드할 수 있습니다. 자세한 내용은 을 IPsec 하드웨어 오프로드 기능 참조하십시오.

ONTAP 9.12.1

MetroCluster IP 및 MetroCluster 패브릭 연결 구성에서 IPsec 프런트엔드 호스트 프로토콜 지원을 사용할 수

있습니다. MetroCluster 클러스터와 함께 제공되는 IPsec 지원은 프런트 엔드 호스트 트래픽으로 제한되며 MetroCluster 인터클러스터 LIF에서는 지원되지 않습니다.

ONTAP 9.10.1

PSK 외에도 인증서를 사용하여 IPsec 인증을 수행할 수 있습니다. ONTAP 9.10.1 이전에는 PSK만 인증에 지원되었습니다.

ONTAP 9.9.1

IPsec에 사용되는 암호화 알고리즘은 FIPS 140-2 검증을 거쳤습니다. 이러한 알고리즘은 FIPS 140-2 검증을 수행하는 ONTAP의 NetApp 암호화 모듈에 의해 처리됩니다.

ONTAP 9.8

IPsec에 대한 지원은 처음에 전송 모드 구현에 따라 사용할 수 있습니다.

IPsec 하드웨어 오프로드 기능

ONTAP 9.16.1 이상을 사용하는 경우 암호화 및 무결성 검사와 같은 계산 집약적인 특정 작업을 스토리지 노드에 설치된 NIC(Network Interface Controller) 카드로 오프로드할 수 있습니다. NIC 카드로 오프로드된 작업의 처리량은 약 5% 이하입니다. 이를 통해 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량을 크게 향상시킬 수 있습니다.

요구 사항 및 권장 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 요구 사항이 있습니다.

지원되는 이더넷 카드

지원되는 이더넷 카드만 설치하고 사용해야 합니다. ONTAP 9.16.1부터 지원되는 이더넷 카드는 다음과 같습니다.

- X50131A(2p, 40G/100G/200g/400G 이더넷 컨트롤러)
- X60132A(4P, 10G/25G 이더넷 컨트롤러)

ONTAP 9.17.1에서는 다음 이더넷 카드에 대한 지원이 추가되었습니다.

- X50135A(2p, 40G/100G 이더넷 컨트롤러)
- X60135A(2p, 40G/100G 이더넷 컨트롤러)

X50131A 및 X50135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K 를 참조하십시오
- AFF A90 를 참조하십시오
- AFF A70 를 참조하십시오

X60132A 및 X60135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A50
- ASA A30

- ASA A20
- AFF A50 를 참조하십시오
- AFF A30 를 참조하십시오
- AFF A20 를 참조하십시오

를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 지원되는 플랫폼과 카드에 대한 자세한 내용은 여기를 참조하세요.

클러스터 범위

IPsec 하드웨어 오프로드 기능은 클러스터에 대해 전역적으로 구성됩니다. 예를 들어, 명령은 `security ipsec config` 클러스터의 모든 노드에 적용됩니다.

일관된 구성

지원되는 NIC 카드는 클러스터의 모든 노드에 설치되어야 합니다. 지원되는 NIC 카드를 일부 노드에서만 사용할 수 있는 경우 일부 LIF가 오프로드 지원 NIC에 호스팅되지 않으면 페일오버 후 성능이 크게 저하될 수 있습니다.

다시 재생 안 함

ONTAP(기본 구성) 및 IPsec 클라이언트에서 IPsec 재생 방지 보호를 비활성화해야 합니다. 비활성화하지 않으면 조각화 및 다중 경로(중복 경로)가 지원되지 않습니다.

ONTAP IPsec 구성이 기본값에서 재생 방지 보호를 사용하도록 변경된 경우 다음 명령을 사용하여 사용하지 않도록 설정합니다.

```
security ipsec config modify -replay-window 0
```

클라이언트에서 IPsec 재생 방지 보호가 해제되어 있는지 확인해야 합니다. 재생 방지 보호를 비활성화하려면 클라이언트에 대한 IPsec 설명서를 참조하십시오.

제한 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 제한 사항이 있습니다.

IPv6를 참조하십시오

ONTAP 9.18.1부터 IPsec 하드웨어 오프로드 기능에 IPv6가 지원됩니다. ONTAP 9.18.1 이전에는 IPsec 하드웨어 오프로드가 IPv6를 지원하지 않았습니다.

확장 순서 번호

IPsec 확장 시퀀스 번호는 하드웨어 오프로드 기능에서 지원되지 않습니다. 일반적인 32비트 시퀀스 번호만 사용됩니다.

Link Aggregation

ONTAP 9.17.1부터 IPsec 하드웨어 오프로드 기능을 사용할 수 있습니다. "링크 집계 그룹" .

9.17.1 이전 버전에서는 IPsec 하드웨어 오프로드 기능이 링크 집계를 지원하지 않습니다. 다음에서 관리하는 인터페이스 또는 링크 집계 그룹과 함께 사용할 수 없습니다. `network port ifgrp` ONTAP CLI에서 명령을 실행합니다.

ONTAP CLI에서 구성을 지원합니다

ONTAP 9.16.1에서는 아래와 같이 IPsec 하드웨어 오프로드 기능을 지원하도록 기존 CLI 명령 세 개가 업데이트됩니다. 자세한 내용은 를 "ONTAP에서 IP 보안을 구성합니다"참조하십시오.

ONTAP 명령	업데이트
'보안 IPsec 구성 표시'	부울 매개 변수는 `Offload Enabled` 현재 NIC 오프로드 상태를 표시합니다.
`security ipsec config modify`	매개 변수는 `is-offload-enabled` NIC 오프로드 기능을 활성화 또는 비활성화하는 데 사용할 수 있습니다.
`security ipsec config show-ipsecsa`	인바운드와 아웃바운드 트래픽을 바이트 및 패킷으로 표시하기 위해 새로운 카운터 4개가 추가되었습니다.

ONTAP REST API에서 구성 지원

아래에 설명된 대로 IPsec 하드웨어 오프로드 기능을 지원하도록 ONTAP 9.16.1에서 두 개의 기존 REST API 끝점이 업데이트되었습니다.

REST 엔드포인트	업데이트
`/api/security/ipsec`	매개 변수가 `offload_enabled` 추가되었으며 패치 메서드에서 사용할 수 있습니다.
`/api/security/ipsec/security_association`	오프로드 기능에 의해 처리된 총 바이트 및 패킷을 추적하기 위해 두 개의 새로운 카운터 값이 추가되었습니다.

를 비롯한 ONTAP REST API에 대한 자세한 내용은 ONTAP 자동화 설명서 를 "ONTAP REST API의 새로운 기능" 참조하십시오. 에 대한 자세한 내용은 ONTAP 자동화 설명서를 검토해야 "IPsec 끝점" 합니다.

관련 정보

- "보안 ipsec"

ONTAP 네트워크에 대한 IP 보안을 구성합니다

ONTAP 클러스터에서 IPsec 전송 중 암호화를 구성하고 활성화하려면 몇 가지 작업을 수행해야 합니다.

IPsec을 구성하기 전에 반드시 "IP 보안 사용을 준비합니다"검토하십시오. 예를 들어, ONTAP 9.16.1부터 사용 가능한 IPsec 하드웨어 오프로드 기능을 사용할지 여부를 결정해야 할 수 있습니다.

클러스터에서 **IPsec**을 활성화합니다

클러스터에서 IPsec을 활성화하여 전송 중에 데이터가 지속적으로 암호화되고 안전하게 보호되도록 할 수 있습니다.

단계

1. IPsec이 이미 활성화되어 있는지 확인:

   '보안 IPsec 구성 표시'

결과에 "IPsec 사용: 거짓"이 포함된 경우 다음 단계를 진행합니다.

2. IPsec 활성화:

   보안 IPsec config modify -is -enabled true

   부울 매개 변수를 사용하여 IPsec 하드웨어 오프로드 기능을 활성화할 수 `is-offload-enabled` 있습니다.

3. 검색 명령을 다시 실행합니다.

   '보안 IPsec 구성 표시'

   그 결과에는 이제 "IPsec 사용: 참"이 포함됩니다.

인증서 인증을 사용하여 **IPsec** 정책 생성을 준비합니다

인증을 위해 사전 공유 키(PSK)만 사용하고 인증서 인증을 사용하지 않는 경우 이 단계를 건너뛸 수 있습니다.

인증을 위해 인증서를 사용하는 IPsec 정책을 만들기 전에 다음 필수 구성 요소가 충족되었는지 확인해야 합니다.

- ONTAP와 클라이언트 모두 최종 엔터티(ONTAP 또는 클라이언트) 인증서를 양쪽 모두에서 확인할 수 있도록 타사의 CA 인증서가 설치되어 있어야 합니다
- 정책에 참여하는 ONTAP LIF에 대해 인증서가 설치됩니다

ONTAP LIF는 인증서를 공유할 수 있습니다. 인증서와 LIF 간 일대일 매핑은 필요하지 않습니다.

단계

1. 상호 인증 중에 사용되는 모든 CA 인증서(ONTAP 측 CA와 클라이언트측 CA 모두 포함)를 ONTAP 인증서 관리에 설치합니다(ONTAP 자체 서명 루트 CA의 경우처럼).
   - 샘플 명령 *
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. 설치된 CA가 인증 중에 IPsec CA 검색 경로 내에 있는지 확인하려면 를 사용하여 ONTAP 인증서 관리 CA를 IPsec 모듈에 추가합니다 `security ipsec ca-certificate add` 명령.
   - 샘플 명령 *
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. ONTAP LIF에서 사용할 인증서를 생성하고 설치합니다. 이 인증서의 발급자 CA가 이미 ONTAP에 설치되어 있고 IPsec에 추가되어야 합니다.
   - 샘플 명령 *
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

ONTAP의 인증서에 대한 자세한 내용은 ONTAP 9 설명서의 보안 인증서 명령을 참조하십시오.

보안 정책 데이터베이스(SPD) 정의

IPsec은 네트워크에서 트래픽이 흐르도록 허용하기 전에 SPD 항목을 필요로 합니다. PSK 또는 인증서를 인증에 사용하는지에 관계없이 적용됩니다.

단계

1. '보안 IPsec 정책 만들기' 명령을 사용하여 다음을 수행합니다.
   a. IPsec 전송에 참여할 IP 주소의 ONTAP IP 주소 또는 서브넷을 선택합니다.
   b. ONTAP IP 주소에 연결할 클라이언트 IP 주소를 선택합니다.

      클라이언트는 미리 공유된 키(PSK)가 있는 인터넷 키 교환 버전 2(IKEv2)를 지원해야 합니다.

   c. 선택적으로 상위 계층 프로토콜(UDP, TCP, ICMP 등), 로컬 포트 번호, 원격 포트 번호 등 트래픽을 보호하기 위한 세부적인 트래픽 매개변수를 선택할 수 있습니다. 해당 매개변수는 다음과 같습니다. `protocols` , `local-ports` 그리고 `remote-ports` 각기.

      ONTAP IP 주소와 클라이언트 IP 주소 사이의 모든 트래픽을 보호하려면 이 단계를 건너뜁니다. 모든 트래픽을 보호하는 것이 기본값입니다.

   d. 에 대한 PSK 또는 PKI(공개 키 인프라)를 입력합니다 `auth-method` 원하는 인증 방법에 대한 매개변수입니다.
      i. PSK를 입력한 경우 매개변수를 포함시킨 다음 <enter> 키를 눌러 미리 공유된 키를 입력하고 확인합니다.

         `local-identity`및 `remote-identity` 매개 변수는 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 선택 사항입니다.

      ii. PKI를 입력하는 경우 도 입력해야 합니다 `cert-name`, `local-identity`, `remote-identity` 매개변수. 원격 측 인증서 ID를 알 수 없거나 여러 클라이언트 ID가 필요한 경우 특수 ID를 입력합니다 `ANYTHING`.
   e. ONTAP 9.17.1부터 선택적으로 포스트퀀텀 사전 공유 키(PPK) ID를 입력합니다. `ppk-identity` 매개변수. PPK는 향후 발생할 수 있는 양자 컴퓨터 공격에 대비하여 추가적인 보안 계층을 제공합니다. PPK ID를 입력하면 PPK 비밀번호를 입력하라는 메시지가 표시됩니다. PPK는 PSK 인증에만 지원됩니다.

자세히 알아보세요 `security ipsec policy create` 에서 "ONTAP 명령 참조입니다" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAP와 클라이언트 모두 일치하는 IPsec 정책을 설정하고 인증 자격 증명(PSK 또는 인증서)이 양쪽 모두에 적용될 때까지 IP 트래픽은 클라이언트와 서버 간에 이동할 수 없습니다.

IPsec ID를 사용합니다

사전 공유 키 인증 방법의 경우 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 로컬 및 원격 ID는 선택 사항입니다.

PKI/인증서 인증 방법의 경우 로컬 및 원격 ID가 모두 필수입니다. ID는 각 측의 인증서 내에서 인증되고 확인 프로세스에 사용되는 ID를 지정합니다. 원격 ID를 알 수 없거나 다른 ID가 많을 수 있는 경우 특수 ID를 사용하십시오 `ANYTHING`.

이 작업에 대해

ONTAP 내에서 SPD 항목을 수정하거나 SPD 정책을 생성하는 동안 ID를 지정합니다. SPD는 IP 주소 또는 문자열 형식 ID 이름일 수 있습니다.

단계

1. 다음 명령을 사용하여 기존 SPD ID 설정을 수정합니다.

보안 IPsec 정책 수정

샘플 명령

'보안 IPsec 정책 수정 - vserver_vs1_-name_test34_-local-identity_192.168.134.34_-remote-identity *client.fooboo.com*`

IPsec 다중 클라이언트 구성

적은 수의 클라이언트가 IPsec을 활용해야 하는 경우 각 클라이언트에 대해 단일 SPD 항목을 사용하는 것이 충분합니다. 하지만 수백 또는 수천 개의 클라이언트가 IPsec을 활용해야 하는 경우 NetApp은 IPsec 다중 클라이언트 구성을 사용할 것을 권장합니다.

이 작업에 대해

ONTAP는 IPsec을 사용하여 여러 네트워크의 여러 클라이언트를 단일 SVM IP 주소에 연결할 수 있도록 지원합니다. 다음 방법 중 하나를 사용하여 이 작업을 수행할 수 있습니다.

- * 서브넷 구성 *

  특정 서브넷(예: 192.168.134.0/24)의 모든 클라이언트가 단일 SPD 정책 항목을 사용하여 단일 SVM IP 주소에 연결되도록 하려면 을 지정해야 합니다 `remote-ip-subnets` 서브넷 형식으로 표시됩니다. 또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다.

  > 서브넷 구성에서 단일 정책 항목을 사용하는 경우 해당 서브넷의 IPsec 클라이언트는 IPsec ID 및 미리 공유된 키(PSK)를 공유합니다. 그러나 인증서 인증에서는 그렇지 않습니다. 인증서를 사용할 때 각 클라이언트는 고유한 인증서 또는 공유 인증서를 사용하여 인증할 수 있습니다. ONTAP IPsec은 로컬 트러스트 저장소에 설치된 CA를 기반으로 인증서의 유효성을 검사합니다. ONTAP는 CRL(인증서 해지 목록) 검사도 지원합니다.

- * 모든 클라이언트 구성 허용 *

  소스 IP 주소와 관계없이 모든 클라이언트가 SVM IPsec 지원 IP 주소에 연결되도록 하려면 을 사용합니다

`0.0.0.0/0` 를 지정할 때 와일드카드입니다 `remote-ip-subnets` 필드에 입력합니다.

또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다. 인증서 인증의 경우 를 입력할 수 있습니다 `ANYTHING`.

또한, 가 있는 경우 `0.0.0.0/0` 와일드카드를 사용하는 경우 사용할 특정 로컬 또는 원격 포트 번호를 구성해야 합니다. 예를 들면, 다음과 같습니다. `NFS port 2049`.

단계

a. 다음 명령 중 하나를 사용하여 여러 클라이언트에 대해 IPsec을 구성합니다.

   i. 여러 IPsec 클라이언트를 지원하기 위해 * 서브넷 구성 * 을 사용하는 경우:

      '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip_subnets_ip_address/subnet_-local-identity_local_id_-remote-identity_remote_id_'

   샘플 명령

   '보안 IPsec 정책 생성 - vserver_vs1_-name_subnet134_-local-ip-subnet134_-local_192.168.134.34 /32_-remote-ip-subnets_192.168.134.0 /24_-local-identity_ontaity_-remote-identity_client_side_identity_'

   i. 을(를) 사용하여 여러 IPsec 클라이언트를 지원하도록 모든 클라이언트 구성 * 허용 을 사용하는 경우:

      '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip-subnets_0.0.0.0/0_-local-ports_port_number_-local-identity_local_id_-remote_identity_remote_id_'입니다

샘플 명령

'보안 IPsec 정책 생성 - vserver_vs1_-name_test35_-local-ip-subnets_ipsec_ip_address/32_-remote-ip-subnets_0.0.0.0/0_-local-ports_2049_-local-identity_side_identity_-remote-identity_client_side_identity_'입니다

IPsec 통계를 표시합니다

협상을 통해 ONTAP SVM IP 주소와 클라이언트 IP 주소 간에 IKE SA(Security Association)라는 보안 채널을 설정할 수 있습니다. IPsec SAS는 실제 데이터 암호화 및 암호 해독 작업을 수행할 수 있도록 두 엔드포인트 모두에 설치됩니다. 통계 명령을 사용하여 IPsec SAS 및 IKE SAS의 상태를 확인할 수 있습니다.

> IPsec 하드웨어 오프로드 기능을 사용하는 경우 명령과 함께 여러 개의 새 카운터가 표시됩니다 `security ipsec config show-ipsecsa`.

샘플 명령

IKE SA 샘플 명령:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA 샘플 명령 및 출력:

SECURN IPSEC show -ipsecsa -node_hosting_node_name_for_svm_ip _'

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA 샘플 명령 및 출력:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

관련 정보

- "보안 인증서 설치"
- "보안 ipsec"

저작권 정보

상표 정보